ceding leaf.[9] Whence it also is plain that the movement of the fixed stars is always progressive and never backward. Wherefore judgments are to be based on their motion, that is, progression. So those who suppose a retrogression of the sphere of some degrees are more in accord with the constants of Thebit or Arzachel than with those of the ancients, since the experience of instruments favors the ancients as to progression of the sphere, and since by that path the world will reach its end, namely when that sphere shall have completed another revolution, according to the opinion of the ancients, I mean.

That the fixed stars and planets should be referred to the conjunction of circles and not conversely is clear from the fact that we count hours by the sun which controls the equinox. And instruments are so constructed, and we arrange the houses by hours. Otherwise when the sun is on the meridian, it would be said to be noon at 1 P.M., and the ninth house would be called the tenth, and so judgments would be in confusion.

Be it noted further that according to Walter Odyngton, monk of Evesham, who composed the foregoing table, the Pleiades in A.D. 1301 were in 17° 22′ Taurus, and Aloiok in 11° 20′ Gemini, and Alabor in 4° Cancer. Taking the longitude with respect to the equinox the figure to such a sign is not more than eight.[10]

Columbia University

[9] This table seems missing in Digby 97, where fol. 142v contains figures for movements of the planets which presumably illustrate the preceding *Theorica sphere* of Grosseteste.

[10] Or perhaps, "the figure to such a sign is no longer eight" (non plus figura est ad tale signum 8).

Athanasius Kircher's Universal Polygraphy

BY GEORGE E. McCRACKEN

TO his contemporaries the Jesuit mathematician Athanasius Kircher (1601–1680) seemed a giant among scientists [1] but with the perspective of three centuries his stature has been greatly diminished. Indeed, it is now generally the fashion to deride him; to point out inaccuracies and misconceptions in his works; to blame him for credulity; to call attention to the fact that he still tried to find truth in such outworn subjects as alchemy, astrology, and horoscopy, while failing to appreci-

[1] For biographical details see the articles on Kircher in the standard manuals: *Encyclopaedia Britannica*, 11th ed., XV, 827; *Brockhaus' Konversations-Lexikon* 14th ed., X, 368; *Der Grosse Herder*, VI, 1416; *Lexikon für Theologie und Kirche*, V; Franz Gehring in *Grove's Dictionary of Music and Musicians*, 3rd ed., III, 26; and particularly the longer articles by Erman in *Allgemeine Deutsche Biographie*, XVI (1882) 1–4, and by Adolf Müller in *The Catholic Encyclopaedia*, VIII, 661–2. There are also said to have been prepared the following biographies: a life by one Pfaff (Fulda, 1631); Kircher's autobiography (*P. Athan. Kircheri vita a semetipso conscripta*) edited by Laugenmantel in 1684 and translated into German by N. Seng in 1901; Behlau's *P. A. Kircher, eine Lebensskizze* (Heilgenstadt, 1874); and Karl Brischar's *P. A. Kircher, ein Lebensbild* (Würzburg, 1877 or 1878). On various aspects of Kircher's work see also George McCracken, *A History of Ancient Tusculum* (Washington, 1939), 3; *idem*, "The villa and tomb of Lucullus at Tusculum," *American Journal of Archaeology*, XLVI (1942), 325–340; George Steindorff and Keith C. Seele, *When Egypt ruled the East* (Chicago, 1942), 3; William Romaine Newbold, *The cipher of Roger Bacon* (Philadelphia, 1928), 32; Paul Friedlaender, "Athanasius Kircher und Leibniz," *Atti della Pontificia Accademia Romana di Archeologia*, (serie 3), Rendiconti, XIII (1937), 229–247; *idem*, "Pindar oder Kircher," *Hermes*, LXX (1935) 463–471; *idem*, "Die Melodie zu Pindars erstem Pythischen Gedicht," *Berichte über die Verhandlungen der sächsischen Akademie der Wissenschaften zu Leipzig*, Philol.-Hist. Klasse, LXXXVI (1934) no. 4, pp. 6–11; Joseph Gutmann, *Athanasius Kircher (1602–1680) und das Schoepfungs-und Entwicklungsproblem* (Würzburg, diss., 1938); Karl Sapper, "Athanasius Kircher als Geograph" in *Aus der Vergangenheit der Universität Würzburg: Festschrift* (Berlin-Würzburg, 1932); Oskar Kaul, "Athanasius Kircher als Musikgelehrter," *ibid.*; and Harry Beal Torrey, "Athanasius Kircher and the progress of medicine," *Osiris*, V (1938), 246–275.

ate the value of the newer Copernican astronomy. Credit has even been taken from him for inventions that are regarded as real achievements, while on those few occasions when he receives praise, he gets it grudgingly because the grains of truth are imbedded in much rubbish.

Kircher's work is vitiated by positive and serious faults: he published far too much and he spread his interest over too wide a field of investigation to permit him to become really expert in any of it. We are told by Müller that in the forty-five years Kircher resided in Rome, he published no fewer than forty-four folio volumes, nearly one a year. His complete bibliography [2] includes a total of forty titles. Though when he was in his early forties he was relieved of the necessity of teaching and thenceforth could devote himself exclusively to research, a fact which may explain in part his prolific output, he had already been a teacher of such varied subjects as the classical languages, natural science, ethics, mathematics, Hebrew, and other oriental languages. In his published works he discusses such miscellaneous topics as volcanoes, ethnology, medicine, physics, music, China, oriental languages including Egyptian hieroglyphs and Coptic, and Roman archaeology. A man who could have made himself master of so wide a field would surely have been entitled to be called "Doctor Centum Artium," as Kepler and Harvey are said to have called him.[3]

The purpose of the present article is not, however, to rehabilitate Kircher's scientific reputation but to call attention to one of his works which has not received in modern times the attention which it deserves.

The work in question was first published at Rome in 1663 and is said to have been issued again at Amsterdam in 1680, the year of Kircher's death. While four copies of the first edition exist in this country,[4] I have been unable to locate a single copy of the second edition. Consequently, all statements made in this article apply only to the first edition.[5]

Certain comments need to be made on the title, a remarkable example of the rococo manner. (See figure 1.) The word "polygraphia" was used in the title of the first edition of the earliest printed treatise on cryptography, that by Joannes Trithemius of Trittenheim (1462–1516) which was first published posthumously in 1618.[6] It means, of course, writing in many forms, as Trithemius uses it, or as Kircher prefers, writing in many languages: the distinction will shortly be made clear. "Steganographia" is the earlier word for cryptography and signifies "hidden writing" (from the Greek adjective *steganós*) as opposed to "secret writing" (cryptography).[7] "Syntagmata" are in modern parlance merely systems.

[2] Augustin de Backer, Alois de Backer, and Charles Sommervogel: *Bibliothèque des Écrivains de la Compagnie de Jésus* (Liége and Lyons, 1869–1872), II, under Kircher's name.

[3] By Edwin Misurell in a copyrighted Sunday feature, *The Columbus Dispatch*, January 1938, but Kepler died when Kircher was only twenty-nine, before the Jesuit had moved to Rome from Avignon. Misurell also attributes to Kircher such inventions as air conditioning, movies, player pianos, periscopes, and amplifiers, on the basis of unspecified "rare old documents recently found in obscure German archives."

[4] In the New York Public Library and in the libraries of the Universities of Michigan, Minnesota, and Pennsylvania. I have personally examined the third and fourth of these.

[5] This work is frequently listed among Kircher's books with the following title: *Polygraphia, seu artificium linguarum, quo cum omnibus totius mundi populis poterit quis correspondere.* It is barely possible that this variant title really belongs to the 1680 edition.

[6] See John Eglinton Bailey's article on "Cryptography" in the eleventh edition of the *Encyclopaedia Britannica*, VII, 565–6. The writer of the unsigned article on Trithemius (*ibid.* XXVII, 296) ignores the contribution of Trithemius to cryptography, as does Sir John Edwin Sandys, *A History of Classical Scholarship* (Cambridge, 1908), II, 258–9, 296.

[7] The term "steganography" is now obsolete but it would have been a useful designation for that form of secret writing in which not only is the secret meaning kept unintelligible without the key, but the very fact that it exists is hidden. To readopt it would make it possible to replace the unsatisfactory term "open code" which now, perforce, almost always is applied to cipher systems.

In the first place the book is an early and apparently independent attempt to offer a solution to a problem which in the sixteenth century was beginning to present difficulties, that of the multiplicity of languages which were even then tending to replace Latin as the universal language of learning. Though Kircher composed all his works in Latin, he seems to have been well aware that already in his day there were men of

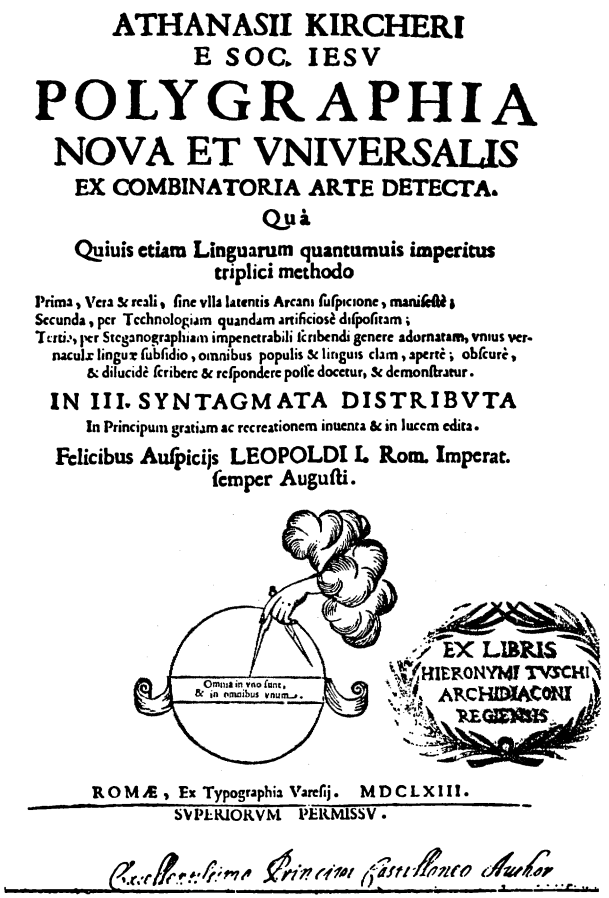

ATHANASII KIRCHERI
E SOC. IESV
POLYGRAPHIA
NOVA ET VNIVERSALIS
EX COMBINATORIA ARTE DETECTA.
Quâ
Quiuis etiam Linguarum quantumuis imperitus
triplici methodo
Prima, Vera & reali, ſine vlla latentis Arcani ſuſpicione, manifeſtè;
Secunda, per Technologiam quandam artificiosè diſpoſitam;
Tertia, per Steganographiam impenetrabili ſcribendi genere adornatam, vnius vernaculæ linguæ ſubſidio, omnibus populis & linguis clam, apertè; obſcurè, & dilucidè ſcribere & reſpondere poſſe docetur, & demonſtratur.
IN III. SYNTAGMATA DISTRIBVTA
In Principum gratiam ac recreationem inuenta & in lucem edita.
Felicibus Auſpicijs LEOPOLDI I. Rom. Imperat. ſemper Auguſti.
Omnia in vno ſunt, & in omnibus vnum.
EX LIBRIS
HIERONYMI TVSCHI
ARCHIDIACONI
REGIENSIS
ROMÆ, Ex Typographia Vareſij. MDCLXIII.
SVPERIORVM PERMISSV.
Excellentiſsimo Principi Caſtellonco Author

FIG. 1. Title-page in the first edition. From the copy in the Library of the University of Pennsylvania (Mendelsohn Collection). Note the autographed presentation of the author and *ex libris* of Tusch.

significance in the history of thought who did not know Latin well enough, and that the newer science then being developed could hardly in every case be expressed by Latin inflections and vocabulary. He had been anticipated in this, but only by two years, in a book by George Dalgarno (*c.* 1626–1687),[8] who in 1661 published his work entitled *Ars Signorum*, an attempt to devise a universal language. Another Englishman, the Bishop of Chester, John Wilkins (1614–1672), was the author of still an-

[8] *Encyclopaedia Britannica*, 11th ed., VII, 764.

other attempt which appeared as an *Essay towards a Real Character and a Philosophical Language* (London, 1668),[9] but neither Dalgarno nor Wilkins was successful.[10]

Kircher certainly owes nothing to Wilkins' book, which came out after the *Polygraphia*, and it is improbable that he had heard of Dalgarno's, for he tells us that he had begun his work on the problem as the result of a suggestion made by Emperor Ferdinand III. We do not know when this suggestion was made but, since Ferdinand died in 1657, Kircher must already have been thinking of the question for at least four years before Dalgarno's book appeared in 1661.[11] The general dissimilarity between the efforts of Dalgarno and Wilkins on the one hand and Kircher's on the other also confirms the view of his independence of the Englishmen. (Kircher's indebtedness to continental precursors will appear as the narrative proceeds.)

The Emperor Ferdinand, so the story goes, had one day been discussing the problem of a universal language and had expressed doubt, well-founded it appears, as to whether the system of cryptography used by Trithemius could be employed for international communication, i. e., communication in two or more languages. Turning to Kircher who was present, he suggested that the latter try his hand at finding an adequate solution; but the problem was difficult — even yet it has not been solved — and the book did not appear until the Emperor who commissioned it had been in his grave for six years. Like its competitors by Dalgarno and Wilkins, Kircher's book is a failure as a solution for the problem of a universal language, but as a contribution to cryptography it should rank high, for it presents, as I believe, the earliest surviving code system, as distinct from cipher systems. The fact that the idea had its *raison d'être* in a search for a universal language is unfortunate since it tended to distract Kircher's attention from the main feature of a cryptographic system, namely, its effectiveness in keeping secret the messages enciphered by it. Moreover, while it cannot be said that cryptographers have overlooked it completely,[12] the fact that many cryptographers nowadays do not read Latin has kept it from being as widely known as it should be.

The volume is divided into two parts, of which the second is an "Appendix Apologetica" of 23 separately-numbered pages. The three systems mentioned in the title are discussed in the first part and are as follows:

a. a polyglot code in five languages;
b. a Trithemian cipher or open code; and
c. a series of substitution ciphers based on a modified Vigenère table.[13]

At the head of his work Kircher prints (2) the following paragraph which summarizes the purpose of the first system:

Syntagma primum

Continet inuentum nouum, quo quisque vel vnica lingua vernacula, qualiscumque tandem illa sit, per litteras, cum omnibus totius orbis populis & Nationibus, reciproco litterarum commercio, correspondere posse demonstratur, & inscribitur: LINGVARVM OMNIVM AD VNAM REDVCTIO.

[9] *Ibid.* XXVIII, 646.

[10] *Ibid.* XXVII, 746–8, *s.v.* "Universal Languages" (Henry Sweet). See also Frederick Bodmer, *The loom of language* (New York, 1944), Chapter XI: "Pioneers of Language Planning" (448–486); Albert Léon Guérard, *A short history of the international language movement* (New York, *c.* 1921). None of the writers cited in this note mentions Kircher's contribution. See also, Clark Emery, "John Wilkins' Universal Language," *Isis*, XXXVIII (1948), 174–185.

[11] That he would in any case have had at this period an opportunity of seeing an English book is unlikely — he shows no knowledge of Francis Bacon's contributions to cryptography.

[12] It is listed, for example, in the bibliography given by A. Lange and E. A. Soudart, *Traité de cryptographie* (Paris, 1925), but without much attention.

[13] For explanation of the cryptographic terminology used in this article see William F. Friedman's fundamental article, "Codes and Ciphers," *Encyclopaedia Britannica*, 14th ed., V, 954–959, reprinted *verbatim* in subsequent editions.

Note that the essential point made here is that the system will reduce all languages to one — there is nothing to suggest that it can be used for secret communications. Though Kircher uses but five languages (Latin, Italian, French, Spanish, and German), he points out that, except for the difficulties encountered in printing, all known languages might be reduced to four basic dictionaries, as follows:

a. Hebrew, Greek, Latin, Italian, French, Spanish, German, Bohemian, Polish, Lithuanian, Hungarian, Belgian, English, and Irish.
b. Chaldaean, Arabic, Armenian, Persian, Turkish, Tartar, and Chinese.
c. Abyssinian and Ethiopian, Nubian, Egyptian, Congo, Angolan, and Bantu.
d. Mexican, Peruvian, Brazilian, Canadian, and other American tongues.[14]

For practical purposes, however, he illustrates the system only in Latin and the four vernaculars which seemed most important to him.

Basically, the system is nothing but a one-part code[15] in Latin, with equivalent values in Italian, French, Spanish, and German, placed in adjoining columns. A one-part code is that type which uses but a single list of the cryptographic symbols called code groups, since when the latter are arranged in alphabetical or numerical order, their corresponding meanings will also be in alphabetical order. A two-part code, on the other hand, is one which is so constructed that the code groups have been assigned to their plain-text values in a mixed sequence, making necessary two lists, one composed of the meanings in alphabetical order for use in encoding, and the other of the code groups in alphabetical or numerical order for use in decoding. It should be obvious that two-part codes are much more secure.

Now it happens that Kircher's code exhibits some of the characteristics of a two-part code, i.e., it needs both an encode and a decode. The reason is to be found in the polyglot nature of the code. Let us consider the decode or "Dictionarium B," as he calls it. This consists of a series of 32 blocks or "pages" (not coterminous with the pages of the book), each numbered by a Roman numeral from I to XXXII and containing from 32 to 40 lines numbered consecutively in arabic numerals. By actual count, the 32 pages contain 1048 groups. On each line there first appears a Latin word and then, in successive columns, the Italian, French, Spanish, and German words which translate the Latin word. For example, block XIII, line 34, is as follows:

magnitudo grandezza grandeur grandeza grösse

In "Dictionarium A," the encode, however, there is no correspondence between the meaning of the words on any line, as will be abundantly clear from the following example:

frigidus IX,35 giungere XII,25 filler XV,8 escasseza XXII,7 Kirche XXII,31

In some instances, one or more of the columns will even lack a word on a given line, because what we have here is five independent lists of the words taken from the decode. It is clear that Kircher prepared his decode first, making each line contain the same idea, though, of course, not the same word, in all the columns. As a result, the encode appears at first glance to be a mixed sequence, whereas it is not. This will be obvious when one considers the Latin column where the encode and decode are identical. Kircher has really produced only a one-part code but the difference in spelling in the four vernaculars has necessitated a separate encode and decode. Were this system to be subjected to cryptanalysis, it would soon be discovered that all the analyst has to do to reconstruct completely a line of the decode already partially recovered in a single column is to find equivalents of the recovered value in the other languages. Thus, the code is truly one-part, being only apparently two-part in character.

[14] The non-European languages currently spoken in those countries.

[15] The difference between a one-part code and a two-part code will be discussed shortly — it is clearly illustrated in Friedman's article cited in note 13.

Though this is true, the principle of alphabeticity is adhered to only roughly, e.g., *aedituus* follows *aegrotatio* in the Latin, but a little search will locate the right word, provided, that is, that Kircher has put it in the code. With only 1048 groups possible, many words will have been omitted. In the main vocabulary (pp. 18–35) some of the plain-text values consist of phrases rather than single words, a feature that looks surprisingly modern, but this, too, is the result of the polyglot character of the code. For example, the Latin phrase *extruere aream lapide quadrato* is found as the equivalent of the French word *paver*. Kircher was not attempting to economize in the number of code groups by making individual groups stand for phrases — he could hardly have anticipated the sending of messages by cable or radio. After the main vocabulary he prints two shorter sections, one (pp. 36–42) containing place names, Christian names (both men and women), adverbs, prepositions, conjunctions, and pronouns, and the other (pp. 42–44) containing the more frequent inflections of the auxiliary verbs *sum* and *habeo*. Here again some of the plain-text values consist of phrases, e.g., a Latin series of the subjunctive of *habeo* (*utinam habeam*, *utinam habeas*, etc.) has an Italian equivalent of *Dio voglia che io habbi*, *tu habbi*, etc. (XXXII, 27ff.).

In striking contrast with this very modern note, however, we find no syllabary or table of special groups used in spelling out words not found in the code, nor are there any groups for this purpose spread through the vocabulary. Consequently, if the word wanted is not in the code, then a synonym must be used instead, and if there is no synonym, the idea simply cannot be expressed. This would have been a very great practical difficulty if the code had ever been put into use, but doubtless any user would have discovered the fact at once and provided a syllabary in a new edition. Kircher himself seems to have vaguely anticipated the difficulty for he advises the reader to cultivate a simple style, devoid of ornate language — if the user doesn't follow this excellent advice, he will find the system useless, for 1048 groups are not enough for ordinary composition.

The code group used in this system is numerical, that is, the cryptographic page or block number is written down in roman numerals, followed by the line number in arabic numerals, e.g., XXX. 10. In nearly all cases there also follows an arbitrary symbol which indicates to the reader the inflectional ending to be supplied to the preceding word. Such signs are lacking only when the vocable is uninflected (e.g., *non*, *ex*, etc.) or when the proper inflection is found in the vocabulary (e.g., *nos*). Now if the primary purpose of the code were to insure secrecy, these signs would constitute a very grave defect for they reveal at once the grammatical skeleton which supports the flesh of the message. Though Kircher was well aware of the possibility of interception, as will be seen from the discussion of the two other systems, he appears to have had no comprehension of the possibility of decipherment of any system without the possession of the keys. Moreover, it is hardly conceivable that the Latin language could have been used in a code of this kind without some indicator of inflection unless the code were so large as to provide for each inflection. This would be prohibitive since the normal Latin verb in full inflection is capable of having 203 different forms.

The arbitrary signs representing the six Latin cases consist merely of the initial letter of the case name, e.g., N = nominative, V = vocative, etc. A = accusative and A = ablative, but the two are distinguished by a small circle at the apex of the first and at the lower right of the second. The circle, incidentally, is used as symbol of the singular while the plural is similarly shown by a straight line or macron. Only three tenses of the verb are provided for: present, perfect, and future. The first is represented by a U-shaped figure; the second by the same figure inverted, while the future is shown by roman numerals, I for first person, II for second person, and III for third. In the other two tenses, person is shown by the number of straight lines at the right. Plurals are indicated by adding a dot except in the case of the future where there is

an upright line at the top right of the figure. Active forms may be converted to passive by drawing a macron over the symbol. There are also more complicated symbols for participles and imperatives, whereas the infinitives appear in the vocabulary and need no symbol. The subjunctive is entirely ignored, except, as has already been stated, in the case of the auxiliary verbs.

Full practical instructions are given (pp. 9–13) for the proper use of this system, together with the following illustration:

Plain-Text: Petrus noster amicus venit ad nos qui portavit tuas litteras ex quibus intellexi animum tuum atque faciam iuxta tuam voluntatem.

Code-Text:[16] xxviii. 36. [n. s.] — xxx. 21. [n. s.] — ii. 5. [n. s.] — xxiii. 8. [3d s. perf.] — xxviii. 10. — xxx. 20. — xxx. 22. — xvii. 29. [3d s. perf.] — xxx. 28. [ac. s.] — xiii. 16. [ac. s.] — xxix. 12. — xxx. 22. [ac. p.] — xii. 3. [1st s. perf.] — xxx. 28. [ac. s.] — ii. 13. [ac. s.] — xxix. 5. — viii. 25. [1st s. fut.] — xxix. 20. — xxx. 28. [ac. s.] — xxiii. 40. [ac. s.].

While the code has obvious defects to which allusion has already been made (its small size, the lack of a syllabary, and the inflectional symbols), here in embryonic form are most of the elements to be found in a modern code system, yet this was devised by Kircher in the seventeenth century. Nothing like it was known prior to his time and it seems not to have been imitated.[17] It constitutes, however, a landmark in the history of cryptography even though its author failed to emphasize its value as a cryptographic system; his primary idea was to provide an easy means of interlingual communication. It was his intention that a reader knowing only one of the five languages could write a message in that language and convert it to code form, and that the recipient knowing only another of the languages, could thereupon read the message with ease in his own tongue. As a sort of afterthought, he points out that there are other uses to which the system can be put, i.e. one can use it as a lexicon and learn, for example, that the German word *grösse* is equivalent to the Italian word *grandezza*, and so on. Finally, the system can be used for secret communications but this to Kircher is the least important use of all.

We now come to the Trithemian cipher (pp. 79–127) which is at once less original and less practical, since it is merely an adaptation of the form of open code invented a century and a half before by Trithemius. Kircher's summary is as follows:

Syntagma Secundum

Continet modum à Trithemio iam olim in sua polygraphia indigitatum, à nemine tamen planè intellectum; quo quiuis, etiam linguarum imperitus, sub qualibuerit lingua, occultos animi sui conceptus amico distanti manifestare queat; & inscribitur, VNIVS LINGVAE AD OMNES ALIAS TRADVCTIO.

Note that here for the first time appears any mention of cryptography: this system is to be used for communicating secrets, but when he criticizes his predecessors for not fully comprehending Trithemius' value, he falls into the same pit, for he does not seem to have realized the fact that the use of such a set of tables greatly hampers the freedom of composition.

Trithemius' cipher was what is now known by the misnomer of "open code." Two messages are involved, one which is intended to be seen by any person who may intercept it and to be taken for the true and only message, but within this is hidden a secret message which only the recipient will know how to read. When properly contrived, such a system is one of the most secure known because its existence is very difficult to

[16] I have here replaced Kircher's arbitrary symbols by their grammatical equivalents within brackets. The original symbols are only a little less easy to read.

[17] Codes did not come into common use until the late eighteenth century and did not become the rule until the nineteenth after the invention of the electro-magnetic telegraph.

detect. But it cannot be said that either in the original form of Trithemius, or in the intermediary form used by Porta (*c.*1538–1615),[18] an adaptation which Kircher imitates more closely than the original of Trithemius, or in the third form of Kircher himself, has the contriving been accomplished with any degree of skill.

Trithemius devised his system so that the cover letter in which the secret message is imbedded forms a theological statement but in both Porta's and Kircher's versions, the cover letter is itself a letter. Kircher provides forty tables for use,[19] each of which should have 22 values, one for each of the 22 letters in Kircher's alphabet (J, K, U, and W are missing) but two pages lack a value for X, one a value for Y, and two, values for Z. These omissions are clearly an oversight on Kircher's part, since, presumably, secret texts might have these letters at the points indicated. Each page contains values of the same general type, so that all cryptograms composed with these tables will have the same form. Since there are only forty tables, a secret text containing more than forty letters will have to repeat some of the tables; likewise, if the text has less than forty, then not all of the tables will have been used, but if the text has exactly forty letters, then the resultant cipher text will be a message of sorts.

Another weakness of the system is that it will produce juxtapositions both semantically, and, probably, syntactically, impossible. The following example, which Kircher sets forth as his illustration of the method, appears to be rather better than most — one suspects that it was first set up and then the tables contrived so as to fit the example, rather than the reverse.

Plain-Text: Cave a latore quia tibi insidiatur.[20]

Cipher-Text: Habui litteras tuas, magnificentissime Theophile, quas mihi tradidit Titus Tabellarius tuus, & simul ac accepi mandata tua, tibi opem ferre volui: nam tui gratiâ, omnibus posthabitis negotijs, Iosepho amantissimo amico tuo tredecim Hungaros expendendos ex dotali pecunia curavi; mando itaque ut hanc inclinationem meam pro pignore habeas, neque enim aliud aveo, nisi ut consanguineos tuos mundo ostendere possim humillima hac virtute mea; quod si aliud quidpiam roges, annue.

I submit that anyone who was asked to carry this letter to Theophilus and took the opportunity to peruse it en route would certainly become exceedingly suspicious that he was carrying a cryptogram, even though he probably would not be able to arrive at the secret meaning, and, if he were such a person as would justify such a warning, he would doubtless be capable of failing to deliver the message at all.

We must now notice an illustration which Kircher inserts between pages 84 and 85 of the book. This purports to represent an "Arca Glottotactica" or linguistic chest.[21] It is a simple box with cubicles for containing strips of wood on which the tables of the Trithemian system have been written. Using the illustration, one may perform the decipherment of the letter quoted above, at least as far as the first three letters of the word "cave" — only three of the tables are actually illustrated. Note that this box is fitted for polyglot tables involving the same five languages used in the first system. Kircher himself had a chest which included Greek, Hebrew, Arabic, Polish, and Persian values, but he omitted these in the drawing for reasons of economy. He was, as we shall see, exceedingly fond of such gadgets as this, but it cannot be said that the *arca* performed any functions which the set of tables alone could not have accomplished as well, and it would be in addition heavy and bulky to carry. Kircher possessed also a set of his tables, lettered on strips in the *arca*, which had the properties of a Vigenère table,[22] that is, instead of using with each strip the same direct standard

[18] J. B. Della Porta, *De Furtivis Litterarum Notis* (Naples, 1563), published precisely a century before Kircher's *Polygraphia*.

[19] Porta prints 57 and Trithemius several hundred.

[20] A melodramatic note.

[21] See Figure 2.

[22] So named from Blaise de Vigenère whose *Traicté des Chiffres* (Paris, 1587) first illustrated this type of square. Note that Vigenère published his beautiful book in French. The typical Vigenère table is illustrated by Friedman in his figure 5.

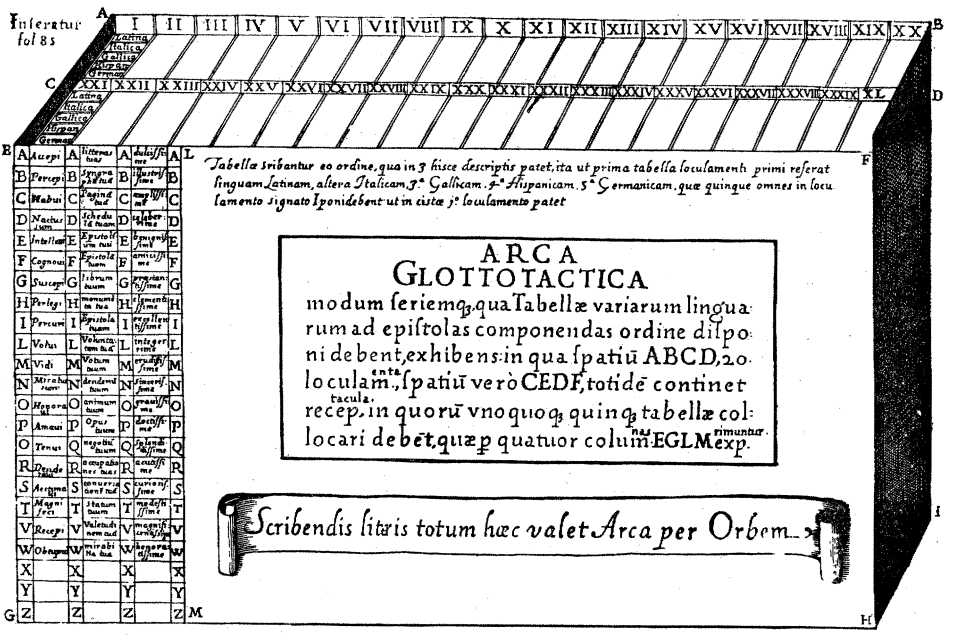


FIG. 2. The "Arca Glottotactica."

alphabet of 22 letters, the second strip would begin with B and have A at the bottom, the third would begin with C and have AB at the bottom, the fourth would begin with D and have ABC at the bottom, and so on. The use of such tables as these would have the effect of combining with the Trithemian cipher a polyalphabetic substitution providing the tables were used in the right way; if not, the only effect would be to jumble the cipher values in a different order and no greater security would be achieved.

The third system, which consists of a series of substitution ciphers, is described in the following summary:

Syntagma Tertium

Nouum continet Arcanum Steganographicum & universale, siue humano ingenio impenetrabilem scribendi modum, qui à Trithemio pariter in sua Polygraphia indigitatur, sed vti in hunc diem à nemine captus, ita quoque passim à plaerisque pro paradoxo habitus fuit, iam tandem à falsa persuasione vindicatus, atque omnibus numeris absolutus in lucem educitur.

Though he attributes the origin of the idea to Trithemius in this summary, Kircher really owes more to Blaise de Vigenère, a sixteenth-century Frenchman who was one of the greatest cryptographers who ever lived,[23] since it was he who first introduced the basic idea of polyalphabetic substitution.

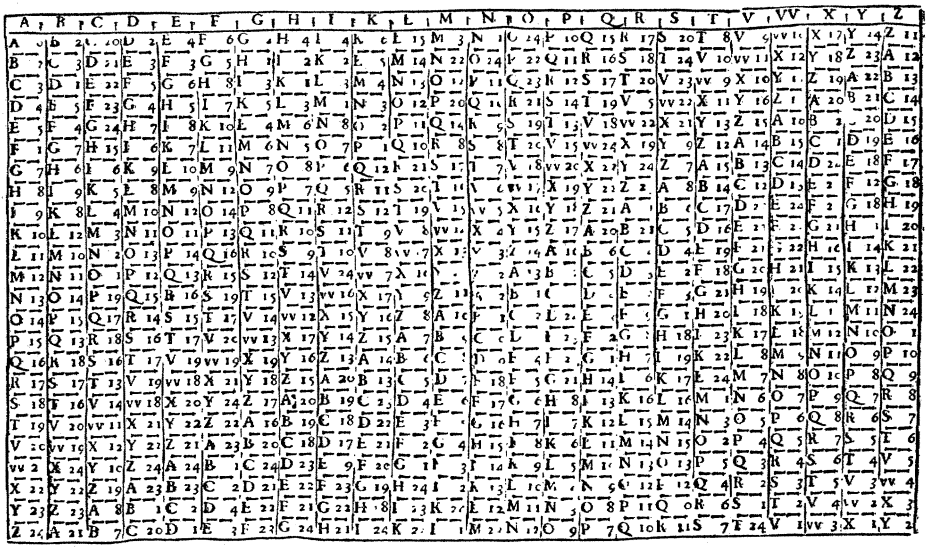
Kircher begins with another gadget, this time an "Arca Steganographica" (p. 130) which embodies the same principles as the "Arca Glottotactica" already described ex-

[23] Yet the *Encyclopaedia Britannica* devotes no article to his memory and even in the article on "Cryptography" (11th edition, VII, 565) he and Porta get only very brief mention as the authors of important treatises. In Friedman's article on "Codes and Ciphers" in the 14th edition, Vigenère gets his just due.

cept that it has only 24 cubicles. This latter chest is in turn based on a Vigenère table (p. 129) which is modified by adding to each column numbers assigned in a mixed, but not thoroughly mixed, sequence.[24] What has been said of the disadvantages of the "Arca Glottotactica" is, of course, equally true of the "Arca Steganographica." Fundamentally, however, all these substitution ciphers may be conveniently described

Pag. 129

Tabulæ Steganographicæ totius Artis combinatiua diſpoſitio.



Hæc Tabula innumeris modis diſponi poteſt: nos hanc præſentem combinationem ſelegimus, iuxta quam tabellæ ſteganographicæ deſcribendæ ſunt.

FIG. 3. A modified "Vigenère" Table.

as variations of the numerical Vigenère table. Kircher's technical name for these variations is "propositiones," a word which doubtless reflects his mathematical training, and there are eight of them, numbered from one to seven, since the learned author overlooks the fact that he has used the number six twice.

First type

The encipherer first chooses one of the columns of the table and enciphers his plain text by setting down in columnar form the numerical values of each plain letter in succession, adding at the beginning some deceptive phrase like "degrees of the sun" to fool the possible interceptor. Somewhere on the sheet, preferably in an inconspicuous place, he writes the letter heading the column chosen.

In the following example the cipher text is transcribed horizontally for convenience: in the original form it is shown vertically.

Plain-Text: Cave ab eo quem non nosti.[25]

Cipher-Text: [key of C]: Degrees of the sun: 20, 8, 14, 22, 8, 7, 22, 1, 17, 14, 22, 3, 2, 1, 2, 2, 1, 16, 13, 6.

Second type

This is like the first except that here two columns are chosen and the numerical values of both are set down with a cover such as "degrees and minutes." The example, using the D and E columns, is based on the same plain text as before:

Cipher-Text: Degrees and minutes: 20, 1; 23, 33; 19, 18; 3, 3; 23, 23; 1, 2; 3, 3; 13, 14; 15, 16; 19, 18; 3, 3; 10, 12; 11, 11; 13, 14; 11, 11; 11, 11; 13; 14; 16, 17; 17, 19; 6, 7.

The columns chosen are here indicated to the addressee by a sentence in which the two key letters D and E, forming the Latin preposition *de*, are capitalized to indicate their significance. The second number of each pair is, of course, redundant: the decipherer needs only to look up the first in the D table and he has the plain text, but the second is transmitted to fool the "enemy" and furnishes a useful correction in case an error has been made. With this varia-

[24] See Figure 3.

[25] Again the melodramatic note.

tion may also be used three-letter keys, e.g. PAX; four-letter keys, e.g. LAVS (Deo); and five-letter keys, e.g. SALVS, all forming parts of pious phraseology which the correspondents might be expected to use, but no matter how long the key, only one letter is necessary and nothing more than simple monoalphabetic substitution is achieved in any case.

Third type

In this variation there is no change from the first type except that here the encipherer sets down the numerals in row. form and uses roman rather than arabic numerals.

Fourth type

Here the tables are used by sliding one column against another, producing nothing but monoalphabetic substitution, a very simple type of cipher to solve. In the example given, two normal alphabets are placed against each other so that a plain A becomes a cipher B, as follows:

Plain: ABCDEFGHIKLMNOPQRSTVWXYZ
Cipher: BCDEFGHIKLMNOPQRSTVWXYZA

Plain-Text: cave ab eo quem non nosti
Cipher-Text: DBWF BC FP RWFN OPO OPTVK

Kircher's printer, however, lacking a W in his type, uses VV for this, and he also sets the line without breaking it into words, thus:

DBVVFBCFPRVVFNOPOOPTVK

Fifth type

The first four types have all been using the table monoalphabetically; this one uses the polyalphabetical method. The first letter of the plain text is enciphered by the first table, the second by the second, and so on, or the encipherer can begin with any table chosen at random and then proceed to the next in order, changing tables with each successive letter. The beginning table must then be revealed to the recipient in some cunning manner but this disadvantage is completely offset by the added security. Kircher realizes this, for he says: "This method is so intricate that no one is of so lofty a genius that in so great a multitude of combinations he can arrive at the meaning of the writer except the one who knows the key; especially, if the key be hidden with singular astuteness." We have here a fair indication of Kircher's attitude towards the possibility of solution without the key. He suggests also that a key word may be used such as IESVS, MARIA, etc. Then the first letter of the plain text is enciphered by the table beginning with I, the second with the table beginning with E, and so on, repeating the key word as many times as necessary. This is really nothing more than the seventh type, discussed below.

Sixth type

This type uses the method now known as "running key."[26] The key is the same length as the plain text. The first of the following two lines (beginning SALVTEM) is the *Key*, while the line immediately under it (beginning CAVEABE) is the *Plain-Text:*

SALVTEM IN EO QVI EST VERA SALVS
CAVEABE OQ VE MHA UDC OGNO VISTI[27]

Then the C is taken from the S table, the A from the A table, and so on. Numerical equivalents would be transmitted and the pious key placed at the end of a meaningless letter.

Seventh type[28]

This is the same as the preceding except that one uses a key phrase not the same length as the plain text and repeats when it has been exhausted. This is really the same as the final suggestion under the fifth type. The same key is S. P. DICIT (=*Salutem plurimam dicit*).

Eighth type

In this variation a letter accompanying the secret text is employed in place of the two different types of running keys illustrated in types six and seven.

After describing these *propositiones* Kircher discusses the use of different languages, a favorite topic with him, to provide keys. He prints a stock letter addressed to "Carissime Theophylacte" which serves as a key and precedes the secret letter. This stock letter is repeated in Latin, Italian, French, Spanish, German, English, Flemish, Greek, Hebrew, and Arabic. The first seven versions are fairly close to one another but the last three are very free translations of the Latin, if, indeed, they are even that close.[29] To serve as an example, I transcribe *litteratim* the English version:

> Knovv that I am very ill content vvith you because that you vvoulde not sende me your booke, I cannott imagine hovv I haue deserued that of you; novv I vvell perceaue you vvill doe very litle for me vvhen you deny me soe small à matter. Your vvords and thoughts doe nott agree vvell one vvith another: if you desired of me things of much greater im-

[26] See Friedman's figure 6.

[27] Note the slight change in the plain text.

[28] Numbered sixth by Kircher.

[29] For reading the Arabic version I am indebted to my friend, Joseph R. Salem; for reading the Hebrew, to my colleague, Dr John C. Trever.

portance: I vvoulde not haue refused them you. It is most true that men commonly say: One ought alvvayes to prooue his freindes before one haue nead of them: for to prooue them in necessity, that vvere to late. Therfore it is enough for mee to haue proued you.[30]

One wonders what the recipient of such a letter would have thought of his correspondent. It seems to have escaped the notice of Kircher that any user of his system might have composed a more sensible letter for himself rather than to use a stock example: perhaps he gives these letters merely to exhibit his prowess in foreign tongues.

It will be remembered that in describing all of the substitutions Kircher has assumed that his reader has made for himself one of the steganographic chests. He now explains that the unfortunate who has not done so may still avail himself of the system by using the printed tables instead, thereby overlooking the point that convenience would have dictated this measure in the first place. He also suggests that the second system (the Trithemian cipher) may be used in the same way as the third, i.e. any six of the Trithemian tables may be taken out and the substitutions applied *à la Vigenère*, but he does not explain beyond saying: "Sagax ingenium facilè meam intentionem intelliget."

The final cipher of this part of the book is one which is inserted apparently as an afterthought. It is easily the least secure of them all, and consists of the open-code type in which the cipher letters are capitalized and stand in second place in their respective words: [31]

Cipher-Text: aFfectus tVus rRga[32] mE eSt sTabilis, tEner, sTudio, pLenus, sAtagam uT tRibuam rOmae tibi parem.[33]
Plain-Text: FVR EST ET LATRO.

The "Appendix Apologetica" consists of a rambling criticism of some of the claims of Trithemius [34] which are, in the opinion of Kircher, in some instances logically inconsistent; in others, impossible, while a third group have been achieved previously and elsewhere. There is also an amusing story attributed to Porta about an Italian nobleman who, having lost his nose in some regrettable accident, got another by means of plastic surgery, the new flesh having been supplied from the body of a retainer. Why this tale is dragged in is not clear unless it was to show that even the great Porta could err. In the appendix also is what is called a Cryptological Table which consists of four columns of words representing, respectively, parts of the body, virtues, vices, and military terms. Except for the vices, each column consists of an acrostic alphabet. Just how this table was intended to be used, I do not know.

Aures	Amor	Odium	Arma
Barba	Beatitudo	Infelicitas	Barbaries
Caput	Castitas	Luxuria	Captivitas
Dentes	Discretio	Indiscretio	Destructio
Exta	Excellentia	Vilitas	Equitatus
Frons	Fides	Perfidia	Fames
Guttur	Gratitudo	Ingratitudo	Grassatio

[30] Note that the Italian compositors when setting English text "justified" the lines by adding a redundant final e and possibly doubled other final letters. They did not do this with Latin or Italian but, as in this very book, added ems and ens or used a set of special final letters (only a, e, m, and n) with graceful tails of varying length. It is possible, of course, that this is not the proper explanation of the spelling. Kircher may have asked some Englishman in Rome to furnish him with an English translation.

[31] It is possible that Kircher did not intend to call attention to the significant second letters by capitalizing them in actual practice.

[32] A misprint for eRga.

[33] The two final words are nulls, necessary to make sense in the cover.

[34] It should be remembered that Trithemius' book was published posthumously and was afterwards reissued in many different editions.

Humerus	Humilitas	Superbia	Habitus Militaris
Inguen	Iustitia	Iniustitia	Instrumenta Bellica
Lingua	Liberalitas	Avaritia	Latrocinia
Manus	Mansuetudo	Iracundia	Machinationes
Nasus	Necessitas	Contingentia	Necessitates
Oculus	Opera Virtutum	Opera Vitiorum	Occupatio urbium
Pectus	Patientia	Impatientia	Peditatus
Quinque digiti	Qualitas animi	Inhabilitas	Qualitas Capitanei
Renes	Religio	Impietas	Rebellio
Supercilia	Sanctitas	Iniquitas	Strategemata
Tempora	Temperantia	Intemperantia	Tentamenta
Venter	Veritas	Falsitas	Vexationes

The appendix closes with what is the only transposition cipher in the entire volume. This is based on a magic square the sum of which totals 34, as the author takes pains to point out:

AENIGMA STEGANOGRAPHVM
AD LECTOREM

Clauis

	34				
	4	14	15	1	
34	9	7	6	12	34
	5	11	10	8	
	16	2	3	13	
	34				

Arcanum

ta	p	an	Haec
ra	ma	am	ri
sci	cra	sa	io
dam	si	gra	a

By writing down the secret syllables in the square at the right in the order of the numbers in the square at the left, the secret is revealed: HAEC SI GRATA SCIAM MAIORA SACRARIA PANDAM. But the meaning of this enigma is still far from clear. Is the author telling his reader that if success awaits the publication of the *Polygraphia*, he will publish another with even more important systems? I do not know the answer to this question but the publication of the *Polygraphia* had a curious sequel.

Two years [35] after the *Polygraphia* appeared, a book was sent to Kircher by his friend and former pupil,[36] Joannes Marcus Marci (1595–1667) of Cronland, who had been Rector of the University of Prague. The letter which accompanied the book has survived. From it we may deduce the following facts: (1) the book sent to Kircher was a cryptogram; (2) specimens of its writing had already been sent to Kircher by a former unspecified owner in the hope that Kircher would help him decipher it; (3) this former owner died without succeeding in solving the cryptogram; (4) a certain Dr Raphael, identified as tutor of the Emperor Ferdinand III when the latter was King of Bohemia, had told Marci that the book had been bought by the Emperor Rudolph [37] for 600 ducats; and (5) that "he" believed that the manuscript was the work of Roger Bacon. Who this person was is not clear: it may have been Raphael or the Emperor Rudolph — all we have to go on is the single word "putabat" without a noun for subject.

This letter was found about 1912 attached to a manuscript purchased from the owner of a castle in Europe by the late Wilfred M. Voynich. Since this manuscript is a crytopgraphic document, it is reasonable to suppose that it is the very book which

[35] That is, on 19 August 1665. For a photograph, Latin transcription, and English translation of the letter accompanying the book, see William Romaine Newbold, *The cipher of Roger Bacon* (Philadelphia, 1928), 31–33. The photograph shows the year as 1665 quite clearly — Newbold seemed to be in doubt for he gives it as 1665 or 1666.

[36] This in spite of the fact that Kircher was younger.

[37] Evidently Rudolph II (1552–1612).

is mentioned in Marci's letter. Whether the book and letter were received by Kircher is another matter. No reference to the manuscript appears in the Amsterdam Catalogue (1678) of the objects given by Kircher to the museum which still bears his name in the old Collegio Romano in Rome. That Kircher was successful in solving the cryptogram, if, indeed, he ever saw it, no one would maintain, for such a man would have rushed into print with his solution.

Nor has the Voynich manuscript been solved in our time, though more than one has made the attempt and claimed success. Of these, the only "solution" which calls for comment, and this only because of the academic respectability previously enjoyed by the "decipherer," is that of William Romaine Newbold, professor of philosophy at the University of Pennsylvania until his death in 1926. The results of Newbold's studies were first announced in a lecture given on 20 April 1921 before the American Philosophical Society at the College of Physicians and Surgeons in Philadelphia. This lecture was published in the *Transactions* of the College of Physicians and Surgeons for 1921 (431–474), and in 1928 my friend, Professor Roland Grubb Kent of the same University, edited for publication a full account of Newbold's research on this problem. But Newbold's claims have not been accepted,[38] and there is the greatest reason to doubt the attribution to Roger Bacon.[39]

Drake University, Des Moines, Iowa

[38] See John M. Manly's attacks in *Speculum*, VI, 345–391; *Harper's Magazine* for July 1921, 186–197.

[39] See Hugh O'Neill, "Botanical Observations on the Voynich MS" in *Speculum*, XIX (1944), 126. O'Neill has identified the plant shown on fol. 93 of the manuscript as the common sunflower, Helianthus annuus L., which was not known in Europe until seeds were brought from America by Columbus on his second voyage. This seems to have a *terminus post quem* for the manuscript of 1493.

An Account of the Salt Industry at Tzu-liu-ching

Tzu-liu-ching chi

BY LI JUNG

(Introductory Note and Translation By Lien-che Tu Fang *)

INTRODUCTORY NOTE ‡

1. Salt in China

In most agrarian civilizations, salt has been a matter of major concern. Its universal use and the conspicuous manner of its distribution make it a decisive source of government revenue and an ideal article for fiscal management.

China's experience offers no exception to this general rule. The origins of certain North Chinese centers of salt production are associated with the country's legendary

* This translation was made for the Chinese History Project in connection with its work on the Ch'ing dynasty. The Project, under the sponsorship of the University of Washington and in cooperation with Columbia University, is engaged in writing a documentary History of Chinese Society.

‡ The Chinese characters corresponding to the transliterations will be found at the end of the article.